A Secure Template Generation Scheme for Palmprint Recognition Systems

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Saroj Kumar Panigrahy

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Orissa, 769 008, India

May 2008

A Secure Template Generation Scheme for Palmprint Recognition Systems

Thesis submitted in partial fulfillment of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering

by

Saroj Kumar Panigrahy

(Roll- 20606006)

Supervisor

Prof. Sanjay Kumar Jena

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela, Orissa, 769 008, India

May 2008

Department of Computer Science and Engineering
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India.

Certificate

This is to certify that the work in the thesis entitled ***A Secure Template Generation Scheme for Palmprint Recognition Systems*** by ***Saroj Kumar Panigrahy*** is a record of an original research work carried out by him under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of Master of Technology in Computer Science and Engineering in the department of Computer Science and Engineering, National Institute of Technology Rourkela. Neither this thesis nor any part of it has been submitted for any degree or academic award elsewhere.

Place: NIT Rourkela
Date: 30 May 2008

Dr. Sanjay Kumar Jena
Professor, CSE Department
NIT Rourkela, Orissa

Acknowledgment

I am grateful to numerous local and global peers who have contributed towards shaping this thesis. At the outset, I would like to express my sincere thanks to Prof. Sanjay Kumar Jena for his advice during my thesis work. As my supervisor, he has constantly encouraged me to remain focused on achieving my goal. His observations and comments helped me to establish the overall direction of the research and to move forward with investigation in depth. He has helped me greatly and been a source of knowledge.

I am very much indebted to Prof. Banshidhar Majhi, Head-CSE, for his continuous encouragement and support. He is always ready to help with a smile. I am also thankful to all the professors of the department for their support.

I express my gratitude to Prof. Pankaj Kumar Sa for generously sharing his time and knowledge and for making life fun while working, just like a friend.

I am really thankful to my all friends. My sincere thanks to everyone who has provided me with kind words, a welcome ear, new ideas, useful criticism, or their invaluable time, I am truly indebted.

I must acknowledge the academic resources that I have got from NIT Rourkela. I would like to thank administrative and technical staff members of the Department who have been kind enough to advise and help in their respective roles.

Last, but not the least, I would like to dedicate this thesis to my family, for their love, patience, and understanding.

Saroj Kumar Panigrahy

Abstract

With the development of more and more systems which provide service based on the identity of a person, the importance of personal identification is growing. Providing authorized users with secure access to the services is a challenge to the personal identification systems. There are several conventional means for personal identification which include passports, keys, tokens, access cards, personal identification number (PIN), passwords. Unfortunately, passports, keys, access cards, tokens, can be lost, stolen or duplicated, and passwords, PINs can be forgotten, cracked or shared. These drawbacks cause a great loss to the concerned. Biometric systems are proving to be an efficient solution to this problem.

A biometric identity verification system tries to verify user identities by comparing some sort of behavioral or physiological trait of the user to a previously stored sample of the trait. The recent developments in the biometrics area have lead to smaller, faster and cheaper systems, which in turn has increased the number of possible application areas for biometric identity verification.

Palmprint can be one of the biometrics, used for personal identification or verification. As a small central part of the palmprint image is used for this purpose, so it is important to find that region of interest. We propose a rotation and translation invariant preprocessing scheme which finds the central part of the palmprints.

As biometric systems are vulnerable to replay, database and brute-force attacks, such potential attacks must be analyzed before they are massively deployed in security systems. Along with security, also the privacy of the users is an important factor as the constructions of lines in palmprints contain personal characteristics. We propose a cryptographic approach to encrypt the palmprint images by an advanced Hill cipher technique for hiding the information on the palmprints. It also provides security to the palmprint images from being attacked by above mentioned attacks. So, during the template generation, the encrypted palmprint sub-images are first decrypted and then the features are extracted.

Contents

List of Figures

Chapter 1

Introduction

Chapter 1

Introduction

As our everyday life is getting more and more computerized, automated security systems are getting more and more importance. Today most personal banking tasks can be performed over the Internet and soon they can also be performed on mobile devices such as cell phones and PDAs. The key task of an automated security system is to verify that the users are in fact who they claim to be. There are three main methodologies when performing this verification. The security system could ask the user to provide some information known only to the user, it could ask the user to provide something only the user has access to or it could identify some sort of trait that is unique for the user. Of course, some sort of combination of these methodologies is also possible.

The first approach, asking for some personal information such as a password, is the classical approach. It has been used for decades in computer systems, but unfortunately this methodology has a major drawback. The problem is related to how the human memory works and what is demanded of a password for it to be considered secure. For a password to be considered secure, an imposter should not be able to guess the password within a reasonably large number of attempts. This means that it should be randomly chosen and of a certain minimum length. Unfortunately studies have shown that this secure length is longer than seven digits [1], which makes passwords hard to remember since humans usually only can hold five to nine digits in their short-term memory at any one time [2].

The second approach, asking for some personal belonging such as a smart card, has also been used for a number of years, for example when accessing high security

facilities. This methodology also has a major drawback, since what is identified by the security system is not the user but actually the belonging. For example, if an imposter steal an authorized user's access card and try to enter a restricted area, there is no way for the security system to know that it is giving access to an imposter and not the user. Of course the method can be combined with a password to get around this problem but then the previously mentioned password problem will be introduced instead.

The third approach, identifying some trait that is unique for the user, is known as biometric security and it is an attempt to get around the previously mentioned problems. A biometrics system is a pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by a user.

1.1 Biometrics

Biometrics is the study of automated methods for recognizing a person based on his physical or behavioral characteristic. Biometric systems can be divided into two categories- identification systems and verification systems. Identification systems tell "who you are?"and verification system tell "are you the one who you claim to be?".

The idea of biometric identification is very old. The methods of imprints, handwritten signatures are still in use. The photographs on the identification cards are still an important way for verifying the identity of a person. But developing technology is paving the way for automated biometric identification and is now a highly interested area of research.

There are different human traits that can be used by a biometric system. Many human characteristics proposed as biometric traits have both advantages and disadvantages. The following parameters are used to decide whether a human trait can be used as a biometric or not.

- ***Universality*** is how common the trait is found in each individual
- ***Uniqueness*** is how well the trait separates an individual form other

- ***Permanence*** is how the trait changes with age
- ***Collectability*** is how easy it is to acquire the trait
- ***Performance*** indicates the accuracy, speed, and robustness of the biometric system built using the trait.
- ***Acceptability*** indicates the degree of approval of a technology by the public in everyday life.
- ***Circumvention*** is how easy it is to fill the authentication system.

1.2 Biometric Technologies

Biometric systems use different physiological and/or behavioral traits of an individual for verification/identification. Different biometric traits have different characteristics and potential applications. There are two types of biometric methodologies: physiological and behavioral. Figure 1.1 shows some of the most used biometric characteristics and the category into which they fall. Physiological methods try to identify the user by some sort of physical trait that is typical to the user. Examples include fingerprint, face, iris, retina etc. On the other hand, behavioral try to identify a user based on some sort of behavior that is typical for a user like the way they walk, or the way they hold the pen while writing or the way they press the keys while entering the PIN etc.

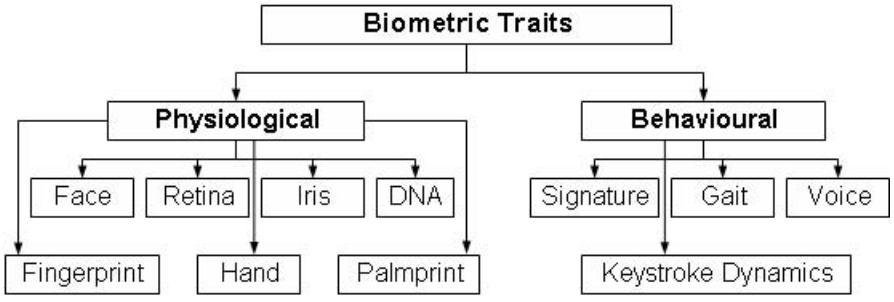

Figure 1.1: Different Biometric Traits

Given below are some of the biometric technologies including those which are still at the research stage.

1.2.1 Fingerprint Authentication

Fingerprint identification has drawn considerable attention over the last 25 years. Fingerprint is used for the identification and considered one of the most reliable and unique characteristic for identification. It is being used from the time when people did not know how to write. Biometric systems based on fingerprint authentication [3] are very popular, reliable and accurate. Fingerprint technology can be used for both verification (1:1) matching as well as for Identification (1:n) matching. The most popular methods of fingerprint authentication are based on minutia features and general fingerprints patterns [4]. The problem with these systems is the difficulty to collect samples as contact with sensor is required to take the fingerprints which can be unhygienic. Also, some people do not have clear fingerprints because of their physical work or problematic skin. Also as the fingerprints are used for legal procedures people hesitate to give their fingerprints.

1.2.2 Palmprint Recognition

The palmprint of a person can be also taken as a biometric as different persons have different palmprints. A palmprint scanner is used to scan the palm and store in a database. A digital camera can also be taken as an image acquisition device for collecting samples of palmprints from a person in different ways. Line features and Texture analyses are used for feature extraction for palmprint verification or identification [5–11].

1.2.3 Face Recognition

Face recognition is a Biometric technology that uses an image or series of images either from a camera or photograph to recognize a person. It does not require a person's cooperation. Face recognition is completely oblivious to differences in appearance as a result of race or gender differences and is a highly robust Biometrics. However, the face changes considerably with age, and even due to make-up and expression changes. Face recognition systems can be divided into two main categories. Systems used to verify the identity of a person in a known

environment at a fairly constant distance and systems that try to identify a person from a group of people in a dynamic environment and at a random distance [12,13].

1.2.4 Retina Scanning

The retina is the layer of blood vessels at the back of the eye. The biometric technology based on retinal scanning is known for low FAR and have therefore been used for years in very high security facilities. But it requires considerable cooperation from the subject as it is inconvenient as intrusive. The retinal scanner requires that the subject should stand still during the scanning process.

1.2.5 Iris Recognition

The iris at first seems to be a bad choice for a biometric. But if observed closely, it has considerable texture detail that makes it a good biometric trait. Iris recognition is considered to be the most accurate biometric technology and is being used very effectively all over the world. Iris recognition technology is safe, accurate and works with high speed without sacrificing accuracy [14, 15].

1.2.6 Ear Recognition

Ear is a relatively new class of biometrics. It has been suggested by the researchers that the shape and features of ear are unique for each person and invariant with age, which has made ear a biometric trait. Several approaches such as two-stage scale and rotation invariant geometric approach which is based on the concept of max-line, the longest line that has both its end points on the edges of the ear, have been proposed for ear recognition [16].

1.2.7 Hand Geometry

Hand Geometry is also one of the most famous biometric. There are two types of hand geometry based systems. One type uses the entire hand for recognition and another type uses only two fingers. It is based on the fact that for every person hand is shaped differently and it does not change significantly with time. The shape and length of the fingers and knuckles are used. Hand recognition systems

are especially useful in outdoor environments and it also has the advantage that the templates are very small in size as small as 9 bytes [17].

1.2.8 DNA Matching

DNA stands for Deoxyribo Nucleic Acid and is found in every cell of an individual. It is completely unique for every person and is most reliable when a positive identification is required. But as it requires extensive testing, it is not the most cost efficient biometric trait.

1.2.9 Voice Recognition

Voice recognition systems work by analyzing the waveforms and air pressure patterns produced while a person talks. These systems may use the characteristics of an individual voice or some pre-arranges words. Voice is one of the most convenient biometric but is not reliable due to bad accuracy. Voice can be mimicked and also a person with a cold or throat problems may face problems using the voice recognition system as it may be rejected [18].

1.2.10 Signature Verification

The handwritten signature is a behavioral biometric. Signatures have been used to verify transactions for centuries and are therefore a well-established method. Automatic signature verification systems do not only examine the appearance of the signature, they also examine the dynamics of the writing. How hard is the pencil pressed against the surface during different phases of the signature? How fast are the different letters written? How long time does it take to write the whole signature? How and when is the letter "t" crossed? There are also several more behavioral biometrics that can be used to verify a user identity using signatures [19].

1.2.11 Keystroke Dynamics

Keystroke dynamics is a very new technology and can be said as an extension to passwords and PINs. It is a behavioral biometric. It works by analyzing the way

one types the keys, the factors like, the time taken by the user to find the keys, the speed of typing. But the method is sensitive to the mood of the user. And the typing dynamics all change as the user is used to typing [20].

1.3 A Typical Biometric System

A Biometric system consists of three parts:

- ***Input Device:*** An input device such as scanner, writing pad etc. These are used to record the inputs which are then used by the software part.
- ***Biometrics Software:*** A software to process the input and convert into digital form, extract the features, and compare the result. In terms of accuracy, the performance of a biometric system completely depends on the quality of the software.
- ***Database:*** A database to store the mathematical information further used for comparison. Features extracted from input samples are stored instead of input samples as the samples take more space and storing features saves the time for processing samples again to extract the features.

The performance of the software is the most important part of a biometrics system as the accuracy of the system depends on the quality of the software. Hence, our main focus is on the software part. The two main processes involved are enrollment or registration, verification and identification. Figure 1.2 shows the architecture of a general biometrics system.

1.3.1 Enrollment Process

It is otherwise known as registration process. In order to identify an individual, it is necessary to store the individual's characteristic features in a database, which are extracted from the reliable samples of the biometric trait either scanned or recorded using input devices like writing pads. These features are then compared with the features extracted from the traits of the individual need to be identified. In order to extract features, the input sample is preprocessed and feature

extraction algorithms are applied on these preprocessed samples to form features vectors. Instead of input samples these feature vectors are stored in the database as input samples take more space on secondary memory than mathematical data and features are computed just once which saves a lot of processing time. A classifier is trained using these feature vectors which then classifies the unknown input sample. For better recognition rate multiple samples for each individual are collected during registration.

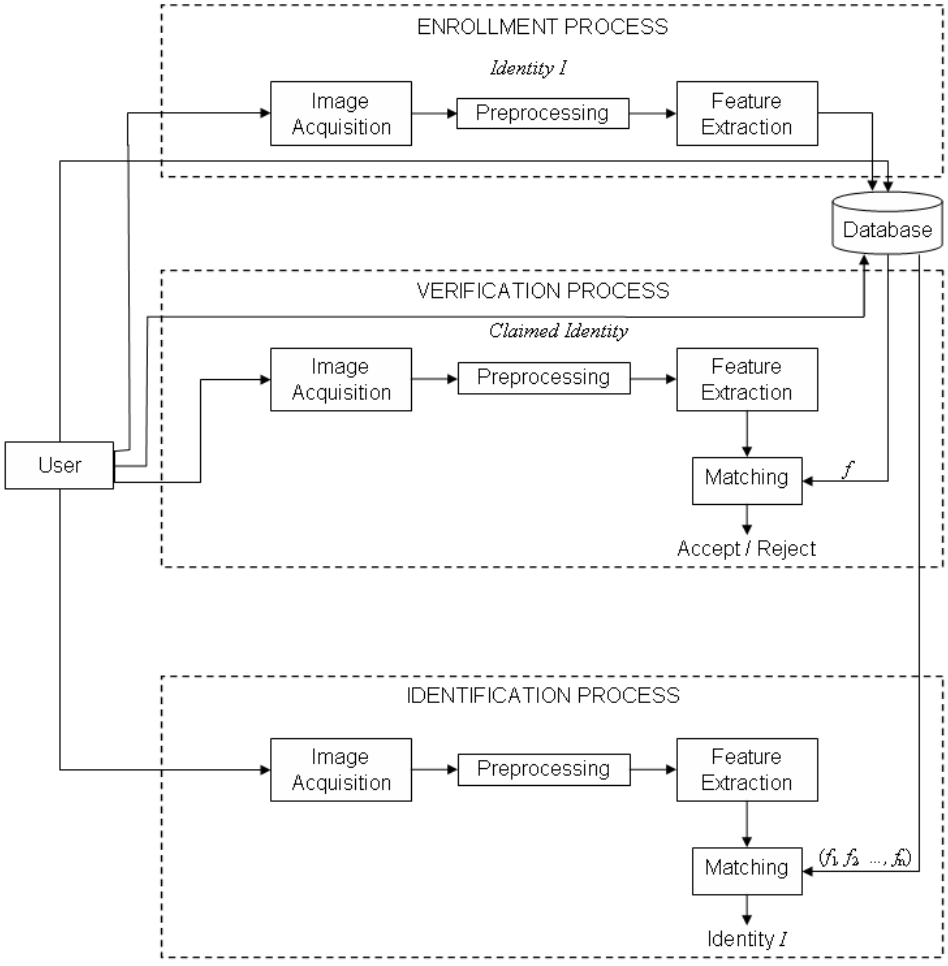

Figure 1.2: Biometric System Architecture

1.3.2 Verification Process

For the verification, same set of features which have been extracted during registration process are extracted from the input samples scanned or recorded using input devices like writing pads, to form the feature vectors. Verification is 1 to 1 matching. In verification, the individual claims his/her identity which is verified by comparing these feature vectors by the feature vectors of the individual which he/she claimed to be. If the matching score crosses the threshold (determined experimentally) then the system verifies the individual as authentic user, else the system rejects the individual.

1.3.3 Identification Process

For the identification also, same set of features which have been extracted during registration process are extracted from the input samples scanned or recorded using input devices like writing pads, to form the feature vectors. Identification is 1 to n matching. In identification, the feature vectors of the individual are compared with the feature vectors of every individual stored in the database. If the highest matching score crosses the threshold (determined experimentally), then it identifies the individual as the person whose matching score is the highest; otherwise the system suggests few top most matches.

1.4 Performance Measures

Various factors such as environmental variations, noise, quality of the input devices etc which makes it very unlikely to get same values of the features extracted from the different samples of the same person at different point of time. Therefore, matching algorithm is needed to compare the samples and computes the matching score and decide if two samples belong to the same individual or not by comparing the matching score against the acceptance threshold. However, it is possible that sometimes the output of a biometrics system may be wrong. Therefore, the performance of a biometrics system is measured in terms of two errors: false accept ratio (FAR) and false reject ratio (FRR).

False Accept Rate (FAR): False acceptance is the number of times the system accepts an unauthorized user and FAR is the ratio of the false acceptance to the number of times the system is used for identification.

False Reject Rate (FRR): False rejection is the number of times the system rejects an authorized user and FRR is the ratio of the false rejection to the number of times the system is used for identification.

These two factors are closely related as both depend on the acceptance threshold which is set to achieve the desired security level. If threshold is set to a very high value then false accept rate of the system may decrease but it may increase false reject ratio and a low threshold may result in decrease in false reject ratio but it may increase the false accept rate. So, the threshold is set according the requirement whether a low FAR or a low FRR is needed.

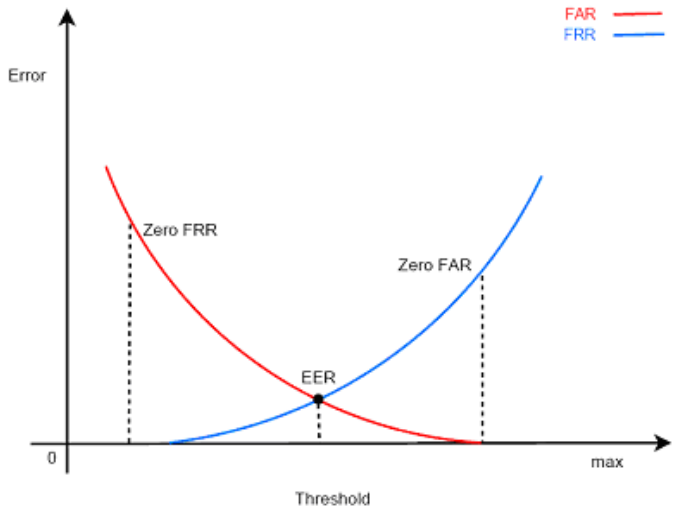

Figure 1.3: A Typical Performance Curve

Equal Error Rate (EER): It is the point where false accept rate and false reject rate are equal. The relation between FAR and FRR can be seen in the Figure 1.3. Aim is to reduce the area obtained by these two curves along the x-axis so it is better choice to set the threshold according to the value of EER

but this is not always preferred. Depending upon the application of biometric system, value of the threshold is set. For example, in a high security application like access to secret government documents, a few rejection of genuine user can be tolerated but it is not desired to give access to any unauthorized user. Therefore, in this case, the threshold is set to a high value to minimize the value of FRR. For another example in an ATM, it is better to risk few false accepts rather than the annoyance of the customers if the system rejects authorized users.

Therefore, for effective comparison of the different biometrics systems, receiver operating characteristics or receiver operating curve (ROC) is used because it is independent of the threshold. In terms of signal theory, ROC is represented by plotting the ratio of true positives vs true negatives. In context of biometrics, it is the graph of genuine acceptance rate plotted against false acceptance rate as shown in Figure 1.4. A point in upper left corner in the ROC space represents the ideal ROC curve i.e. 100% genuine acceptance rate and no false acceptance.

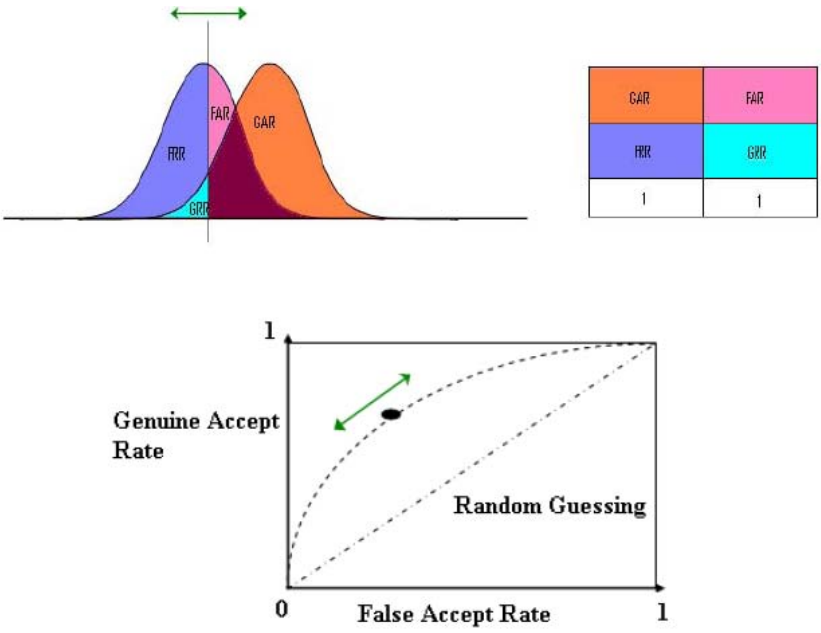

Figure 1.4: Receiver Operating Characteristics

There are other issues as well to be considered when evaluating a system's performance, such as time. For example one cannot use a biometric system in an ATM if it takes several minutes to verify a user.

1.5 Problems Raised by Biometrics

In addition to the potential illegitimate access by imposters, biometric systems raise issues including unintended functions, unintended applications and template sharing.

- **Unintended Functions:** Our biometric traits contain rich private information, which can be extracted from biometrics for non-authentication purposes. DNA containing all genetic information including sex, ethnicity, physical disorder and mental illness can be employed for discrimination. Certain patterns in palm lines also associate with mental disorders such as Down syndrome and schizophrenia.

- **Unintended Applications:** Some biometric traits can be collected without user cooperation. Face and iris are two typical examples. Governments and organizations can employ them for tracking.

- **Template Sharing:** Biometric templates in databases of authorized agents are possible to be shared by unauthorized agents.

1.6 Problem Formulation

After the palmprint images are collected, the preprocessing of those palmprint images is one of the important phases in palmprint recognition systems. Instead of the large palmprint image, a small central sub-image is required for feature extraction. So, in the preprocessing scheme, the central region of interest (ROI) is extracted from the large palmprint image. Also sometimes, the palmprint images need enhancements. During the enrollment phase, multiple samples of palmprints per user are collected in regular intervals. So each time the user puts his/her palm on the space provided in the scanner, the palm's position suffers from a little bit of rotation and translation. So, the central ROI generated each time will be different. But we require the central sub-images generated from the preprocessing phase should be all similar.

We have proposed a preprocessing scheme for generating the central palmprint sub-images by considering the centre of gravities of the two holes generated by the fingers, which is proved to be rotation as well as translation invariant scheme, i.e., even if the palms are rotated through a small angle and translated a little, our scheme is able to generate the similar palmprint sub-images.

Biometrics is much more secure than traditional authentication methods. But, they are not, however, invulnerable. For example, they are open to database, replay, and brute-force attacks. We have proposed an encryption technique to encrypt the palmprints for maintaining privacy of the palmprints and also generated palmprint sub-images by a modified version of Hill cipher algorithm, before transmitting to the remote system for storing in database for future use. Our scheme resists the brute-force attacks and database attacks to palmprint sub-images.

1.7 Motivation

Fingerprint identification has drawn considerable attention over the last 25 years. However, some people do not have clear fingerprints because of their physical work or problematic skin. Iris and retina recognition provide very high accuracy but suffer from high costs of input devices or intrusion into users. Recently, many researchers have focused on face and voice verification systems; nevertheless, their performance is still far from satisfactory. The accuracy and uniqueness of 3-D hand geometry are still open questions. Compared with the other physical characteristics, palmprint authentication has several advantages: (a) low-resolution imaging; (b) low intrusiveness; (c) stable line features and (d) high user acceptance. It is obvious that on-line identification is more important for many real-time applications, so that it draws our attention to investigate.

Biometric authentication systems are widely applied because they offer inherent advantages over classical knowledge-based and token-based personal identification approaches. However, biometric systems are vulnerable to various attacks; such potential attacks must be analyzed before biometric systems are massively deployed in security systems. Also very less works have been done for the security

of the biometric templates.

Cryptography is one possible solution that would allow us to better defend against replay and database attacks. Systems protected by cryptography store and transmit only encrypted templates in databases and through data links. However, cryptography is not suitable for speed-demanding matching, e.g. real-time large-scale identification, since decryption is required before matching. Another potential solution is cancellable biometrics. Cancellable biometrics transform original templates into other domains and perform matching in the transformed domain. Although cancellable biometrics overcome the weakness of cryptography, current cancellable biometrics are still not secure enough for the palmprint identification. Also the original palmprints cannot be reconstructed from the cancellable biometric templates. This attracts our attention to work in the area of cryptography for providing security to palmprint images.

1.8 Thesis Organization

The rest of this thesis is organized as follows.

In Chapter 2, an overview of typical palmprint recognition systems are discussed. Here all the phases: *Palmprint acquisition*, *Preprocessing*, *Feature Extraction*, and *Matching* of a palmprint recognition system are explained. Then it discusses the privacy and security issues involved with it. It also discusses various literatures surveyed related to the work.

Chapter 3 proposes a palmprint preprocessing scheme based on the centre of gravity of the holes created by the fingers. It also proposes a secure scheme of encrypting the palmprint images by a advanced version of Hill Cipher before transmission in networks and storage in remote databases and maintains privacy of the palmprints of the users. It also discusses the simulations and results of our proposed scheme.

Finally, Chapter 4 discusses the concluding remarks with scope for further research work.

Chapter 2

Literature Survey

Overview of Palmprint Recognition Systems

Privacy and Security of Biometric Systems

Other Related Works

Summary

Chapter 2

Literature Survey

Palmprint recognition has been investigated over the past ten years. During this period, many different problems related to palmprint recognition have been addressed. Researchers have focused on developing accurate verification algorithms. Various feature extraction and matching algorithms have been proposed. To achieve high verification accuracy, researchers combine different biometric traits with palmprints and combine different features in palmprints. Researchers also address a more challenging problem, real-time palmprint identification in large databases. In this context, both accuracy and recognition speed are important. Recently, the biometric community has also emphasized on the security of biometric systems. Pioneers have proposed some measures to protect palmprint systems. In addition to summarizing the current palmprint research, other related issues like privacy involved with palmprints are discussed. The aims of this chapter are to give an overview of the current palmprint research.

2.1 Overview of Palmprint Recognition Systems

Palmprint, the inner surface of our palm normally contains three flexion creases, secondary creases and ridges. The flexion and secondary creases are also called principal lines and wrinkles, respectively. The flexion creases and the main creases are formed between the 3rd and 5th months after conception and superficial lines appear after birth. These creases are not genetically deterministic. Even identical twins who share the same DNA sequences have different palmprints. These non-

genetically deterministic and complex patterns have rich information for personal identification.

There are two types of palmprint recognition research, high resolution and low resolution approaches. High resolution approach employs high resolution images while low resolution approach employs low resolution images. High resolution approach is suitable for forensic applications such as criminal detection, while low resolution is more suitable for civil and commercial applications such as access control. Generally speaking, high resolution refers to 400 dpi or more and low resolution refers to 150 dpi or less. Figure 2.1 illustrates a part of a high resolution palmprint image and a low resolution palmprint image. In high resolution images, researchers can extract ridges, singular points and minutia points as features while in low resolution images, they generally use principal lines, wrinkles and texture. At the beginning of palmprint research, the high-resolution approach was the focus but almost all current research is focused on the low resolution approach because of the potential applications. In this chapter, we concentrate only on the low resolution approach since it is the current focus.

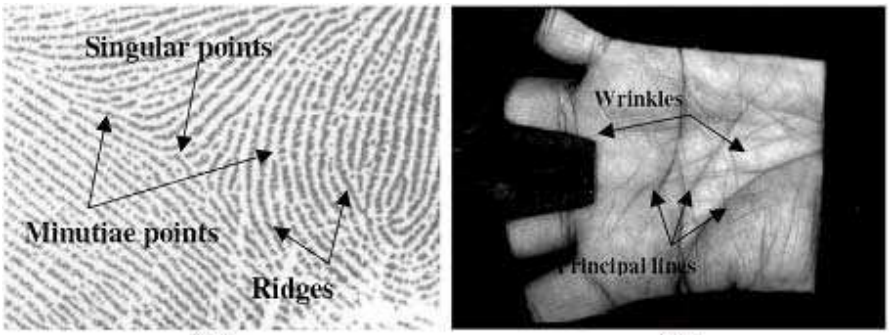

Figure 2.1: Palmprint features in (a) a high resolution image and (b) a low resolution image

A palmprint recognition system generally consists of five parts: palmprint scanner, preprocessing, feature extraction, matcher and a database. Palmprint scanner is to collect palmprint images. Preprocessing is to setup a coordinate system to align palmprint images and to segment a part of palmprint image for

feature extraction. Feature extraction is to obtain effective features from the preprocessed palmprints. Finally, a matcher compares two palmprint features. All the images, templates generated are stored in a local or remote database.

2.1.1 Palmprint Image Acquisition

It is the first process in palmprint recognition systems. Researchers utilize four different types of sensors to collect palmprint images, CCD-based palmprint scanners, digital cameras, digital scanners and video cameras. Figure 2.2 shows a CCD-based palmprint scanner developed by the Hong Kong Polytechnic University [21]. Generally speaking, CCD-based palmprint scanners capture high quality palmprint images and align palms accurately since the scanners have pegs for guiding placement of hands. Digital scanners are cost-effective to collect palmprint images. However, they cannot support real-time verification because of the scanning time. Digital cameras and video cameras are two ways to collect palmprint images without contact. Figure 2.3(a) is a palmprint image collected by a CCD-based palmprint scanner and Figure 2.3(b) is a palmprint image collected by a digital scanner.

Figure 2.2: A CCD-based palmprint scanner

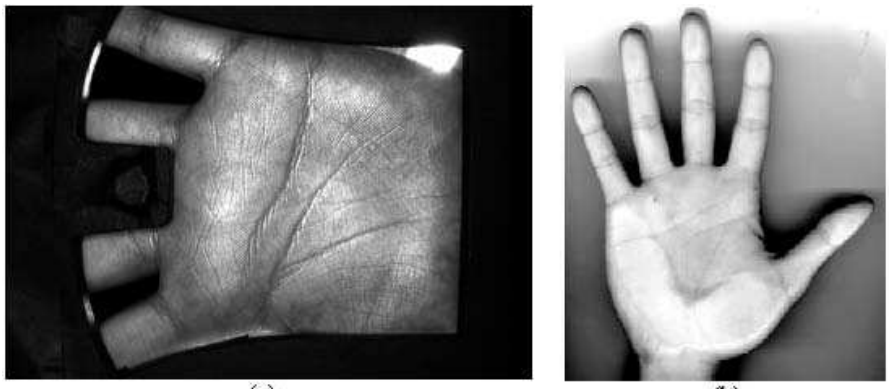

Figure 2.3: Two palmprints collected by (a) a CCD-based palmprint scanner, (b) a digital scanner

2.1.2 Palmprint Preprocessing

Preprocessing is used to align different palmprint images and to segment the central parts for feature extraction. Most of the preprocessing algorithms employ the key points between fingers to set up a coordinate system. Preprocessing involves generally five common steps, (1) binarizing the palm images, (2) extracting the contour of palm and/or fingers, (3) detecting the key points, (4) establishing a coordination system and (5) extracting the central parts. Figure 2.4 (a) illustrates the key points and Figure 2.4 (b) shows a preprocessed image. The first and second steps in all the preprocessing algorithms are similar. However, the third step has several different implementations including tangent-based [21] and wavelet-based [8]. All these approaches utilize only the information on the boundaries of fingers. After obtaining the coordinate systems, central parts of palmprints are segmented. Most of the preprocessing algorithms segment square regions for feature extraction.

2.1.3 Palmprint Feature Extraction

A lot of work has been done for developing feature extraction algorithms. D. Zhang et al. have used datum point and line features for palmprint verification system [5]. Li et al. have used Fourier transform for feature extraction of palmprints [6]. Kong et al. have proposed palmprint feature extraction using 2-D Gabor filters [9]. Gan

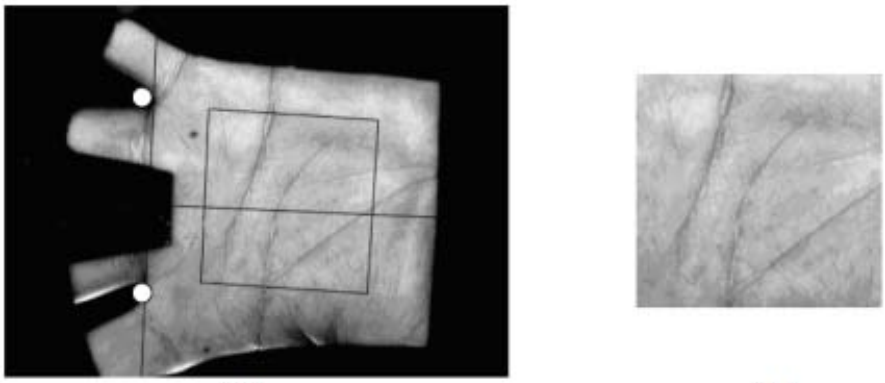

Figure 2.4: Illustration of preprocessing, (a) the key points based on finger boundary and (b) the central parts for feature extraction.

et al. have applied wavelet transform for palmprint recognition [10]. Wu et al. have proposed palmprint texture analysis using Derivative of Gaussian filters [11].

2.1.4 Palmprint Matching

Also there has been lot of works on palmprint matching. Many existing classifiers including neural networks [8], various measures including cosine measure, weight Euclidean distance, Euclidean distance, hamming distance and nearest neighborhood distance have been examined [5–11].

2.2 Privacy and Security of Biometric Systems

Biometric traits contain information not only for personal identification but also for other applications. For example, deoxyribonucleic acid (DNA) and retina are useful for diagnosing genetic problems and diabetes, respectively. Palmprints are also related to some genetic disorders and are used by fortune-tellers or palmists to predict the characteristics of the individuals. To protect the private information in palmprints, databases have to store encrypted palmprint images and also templates only, since the line features are possible to be reconstructed from raw templates.

Given the commercial potential of palmprint systems as security applications, the wide variety of capture devices that now exist, and the diversity of prepro-

cessing, feature extraction, matching and classification algorithms that have been produced in the field, it is certainly the case that any security issues should be systematically addressed prior to their widespread deployment. Palmprint recognition has been studied for many years and the potential attacks have been identified but only limited research work is related to the security of palmprint systems.

Although biometric authentication approaches are much more secure than the traditional approaches, they are not invulnerable. Biometric systems are vulnerable to many attacks including replay, database and brute-force attacks. Comparing verification, fusion and identification, only limited works are related to palmprint security [22]. Figure 2.5 shows a number of points, Points 1-8, all being vulnerable points as identified by Ratha et al. [23]. The potential attack points are between and on the common components of a biometric system, input sensor, feature extractor, matcher and database and are especially open to attack when biometric systems are employed on remote, unattended applications, giving attackers enough time to make complex and numerous attempts to break in. At Point 1, a system can be spoofed using fake biometrics such as artificial gummy fingerprints and face masks. At Point 2, it is possible to avoid liveness tests in the sensors by using a pre-recorded biometric signal such as a fingerprint image. This is a so-called replay attack. At Point 3, the original output features can be replaced with a predefined feature by using a Trojan horse to override the feature extraction process. At Point 4, it is possible to use both brute-force and replay attacks, submitting on the one hand numerous synthetic templates or, on the other, prerecorded templates. At Point 5, original matching scores can be replaced with preselected matching scores by using a Trojan horse. At Point 6, it is possible to insert templates from unauthorized users into the database or to modify templates in the database. At Point 7, replay attacks are once again possible. At Point 8, it is possible to override the system's decision output and to collect the matching scores to generate the images in the registered database.

Both Cryptographic techniques and cancellable biometrics can be used for encryption. The difference between these two approaches is that cancellable bio-

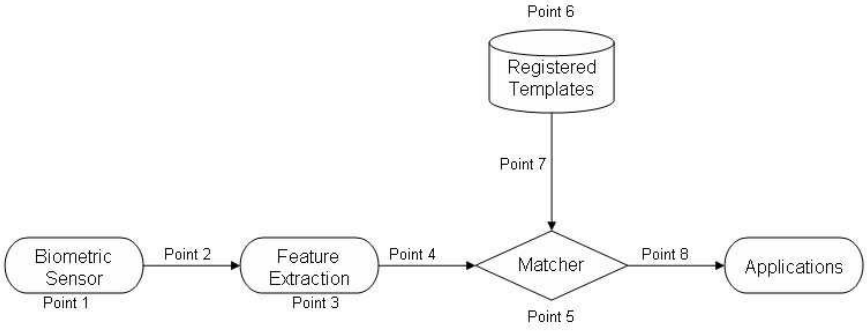

Figure 2.5: Potential attack points in a biometric system

metrics performs matching in transform domains while cryptographic techniques require decryption before feature extraction and/or matching. In other words, decryption is not necessary for cancellable biometrics. When matching speed is an issue, e.g., identification in a large database, cancellable biometrics is more suitable for hiding the private information. And when privacy and security of palmprint database is required then cryptographic techniques can be used for encrypting the palmprint images in the database.

2.3 Other Related Works

This section gives an introduction to some other concepts related to our work.

2.3.1 Hill Cipher Encryption Technique

It is developed by the mathematician Lester Hill in 1929. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher each character is assigned a numerical values like $a = 0,\ b = 1,\ c = 2,\ ...,\ z = 25$ [24]. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equations. For $m = 3$, the system can be described as follows:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3)\ mod\ 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3)\ mod\ 26 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3)\ mod\ 26 \end{aligned} \tag{2.1}$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \tag{2.2}$$

or simply we can write as $C = KP$, where C and P are are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key. All operations are performed *mod* 26 here. Decryption requires using the inverse of the matrix K. The inverse K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix.

But when the key matrix is taken randomly, the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the ciphertext, and then the plaintext is recovered. In general term we can write these as follows:

For encryption:

$$E_K(P) = KP = C \tag{2.3}$$

For decryption:

$$D_K(C) = K^{-1}C = K^{-1}KP = P \tag{2.4}$$

As this technique can be applied to text messages for encryption, similarly also can be applied to encrypt images as images are nothing but the 2-D matrices containing values which are gray levels or colour indices of an image.

2.3.2 Modular Arithmetic

Modular arithmetic (sometimes called *modulo arithmetic* or *clock arithmetic*) is a system of arithmetic for integers, where numbers "wrap around" after they reach a certain value— the *modulus*. Modular arithmetic was introduced by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae*, published in 1801.

Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations of the ring of

integers: addition, subtraction, and multiplication. For a fixed modulus p, it is defined as follows.

$$a \equiv b \bmod p \text{ if } p|(a-b)$$

The congruence modulo operator has the following properties:

1. $a \bmod p = b \bmod p \Rightarrow a \equiv b \bmod p$
2. $a \equiv b \bmod p \Rightarrow b \equiv a \bmod p$
3. $a \equiv b \bmod p$ and $b \equiv c \bmod p \Rightarrow a \equiv c \bmod p$

Let $\mathbb{Z}_p = [0, 1, \ldots, p-1]$ the set of residues modulo p. If modular arithmetic is performed within this set $\mathbb{Z}_p$, the following equations present the arithmetic operations:

- ***Negation:*** $-a \bmod p = p - a \bmod p$
- ***Addition:*** $(a+b) \bmod p = (a \bmod p + b \bmod p) \bmod p$
- ***Subtraction:*** $(a-b) \bmod p = (a \bmod p - b \bmod p) \bmod p$
- ***Multiplication:*** $(a*b) \bmod p = (a \bmod p * b \bmod p) \bmod p$
- ***Division:*** $(a/b) \bmod p = c$ when $a = (b*c) \bmod p$

The following exhibits the properties of modular arithmetic.

- **Commutative Law:**
  $(x+y) \bmod p = (y+x) \bmod p$
  $(x*y) \bmod p = (y*x) \bmod p$
- **Associative Law:**
  $[(x+y)+z] \bmod p = [x+(y+z)] \bmod p$
- **Distributive Law:**
  $[x*(y+z)] \bmod p = [\{(x*y) \bmod p\} + \{(x*z) \bmod p\}] \bmod p$

- **Identities:**

  $(0 + x) \bmod p = x \bmod p$

  $(1 * x) \bmod p = x \bmod p$

- **Inverses:**

  if for $x \in \mathbb{Z}_p, \exists y$ such that $(x + y) \bmod p = 0$, then $y = -x$

  if for $x \in \mathbb{Z}_p, \exists y$ such that $(x * y) \bmod p = 1$, then $y = x^{-1}$

2.3.3 Use of Involutory Matrices

Involutory matrix is a matrix that is its own inverse. That is, matrix A is an involution if $A = A^{-1}$ or $A^2 = I$. As we have seen in Hill cipher, decryption requires inverse of the matrix. So while decryption one problem arises that is, inverse of the matrix does not always exist. Then if the matrix is not invertible, then encrypted text cannot be decrypted. In order to overcome this problem we suggest the use of involutory or self-invertible matrices while encryption in the Hill Cipher.

In the self-invertible matrix encryption method, the key matrix used for the encryption is self-invertible. So at the time of decryption we need not find the inverse of the key matrix. More over this method eliminates the computational complexity involved in finding inverse of the matrix while decryption. There are several methods proposed for generating self-invertible matrices [25]. One of the methods we used in our proposed approach to generate even order key matrices for encryption is presented below.

The analysis presented here for generation of self-invertible key matrix is valid for matrix of +ve integers, that are the residues of modulo arithmetic of a number. This algorithm can generate self-invertible matrices of order $n \times n$ where n is even.

Let $A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{13} \\ a_{21} & a_{22} & \dots & a_{23} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$ be partitioned into four sub matrices $\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$,

where $A_{11},\ A_{12},\ A_{21}$ and A_{22} are matrices of order $\frac{n}{2}\times\frac{n}{2}$ each.

As A is self-invertible, so $A = A^{-1}$ and $A.A^{-1} = I$, i.e.,

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} . \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} = I = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}$$

Then we get,

$$A_{11}^2 + A_{12}A_{21} = I, \tag{2.5a}$$

$$A_{11}A_{12} + A_{12}A_{22} = 0, \tag{2.5b}$$

$$A_{21}A_{11} + A_{22}A_{21} = 0, \tag{2.5c}$$

$$A_{21}A_{12} + A_{22}^2 = I \tag{2.5d}$$

From equation (2.5a) we get,

$A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$

i.e., If A_{12} is one of the factors of $I - A_{11}^2$ then A_{21} is the other.

So, if $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$,

then $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$, where k is a scalar constant.

Then, putting the values of A_{12} in equation (2.5b) we get,

$A_{11}k(I - A_{11}) + k(I - A_{11})A_{22} = 0$

$\Rightarrow k(A_{11} + A_{22})(I - A_{11}) = 0$

$\Rightarrow A_{11} + A_{22} = 0$ or $A_{11} = I$

Since $A_{11} = I$ is a trivial solution, so, $A_{11} + A_{22} = 0$ is taken,

i.e., $A_{11} = -A_{22}$.

When we solve equations (2.5c) and (2.5d), same solution is obtained. Then the main matrix can be formed by appending all the four matrices.

Algorithm: Self-Invertible Matrix Generation

1. Select any arbitrary matrix A_{22} of order $\frac{n}{2}$.
2. Obtain $A_{11} = -A_{22}$.
3. Take $A_{12} = k(I - A_{11})$ or $k(I + A_{11})$ where k is a scalar constant.

4. Then find $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$.

5. Form the matrix A completely by appending all the four matrices $A_{11},\ A_{12},\ A_{21}$ and A_{22}.

Example: (For Modulo 13)

Let $A_{22} = \begin{bmatrix} 10 & 2 \\ 3 & 4 \end{bmatrix}$, then,

$A_{11} = -A_{22} = \begin{bmatrix} 3 & 11 \\ 10 & 9 \end{bmatrix}$

if k is selected as 2, then,

$A_{12} = k(I - A_{11}) = \begin{bmatrix} 9 & 4 \\ 6 & 10 \end{bmatrix}$ and

$A_{21} = \frac{1}{k}(I + A_{11}) = \begin{bmatrix} 2 & 12 \\ 5 & 5 \end{bmatrix}$

So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$ will be the self-invertible matrix.

2.3.4 Enhanced Hill Cipher Techniques

Saeednia S. has proposed a symmetric cipher that is actually a variation of the Hill cipher. His scheme makes use of "random" permutations of columns and rows of a matrix to form a "different" key for each data encryption. The cipher has matrix products and permutations as the only operations which may be performed "efficiently" by primitive operators, when the system parameters are carefully chosen [26].

A main drawback of Hill Cipher algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and cannot encrypt images that contain large areas of a single colour. Thus, it does not hide all features of the image which

reveals patterns in the plaintext. Moreover, it can be easily broken with a known plaintext attack revealing weak security. So, Ismail et al. have proposed a variant of the Hill cipher that overcomes these disadvantages [27]. The proposed technique adjusts the encryption key to form a different key for each block encryption. It is mentioned in the paper that their proposed variant yields higher security and significantly superior encryption quality compared to the original one. But Y. Rangel-Romero et al. have given comments on the above proposed technique that the proposed method of encryption using modified Hill cipher still has security flaws as compared to the original Hill Cipher technique [28].

2.3.5 Some Image Processing Concepts

This section discusses study of some of the image processing concepts which are used in our work.

A. Image Acquisition: Image acquisition is the first step out of the fundamental steps in digital image processing– that is, to acquire a digital image. To do so requires an imaging sensor and the capability to digitize the signal produced by the sensor. The sensor could be a monochrome or colour camera or a scanner. If the output of the camera or other imaging sensor is not already in digital form, an analog-to-digital converter (ADC) digitizes it. The nature of the sensor and the image it produces are determined by the application [29].

For any online palmprint recognition system the palmprint images are collected by a scanner or a digital camera from the palms of the users. In our work, we have not used any scanner or camera for acquiring the palmprint images. We have used the readily available palmprint images from PolyU palmprint database [30].

B. Image Preprocessing: After a digital image has been obtained, the next step deals with preprocessing that image. The key function of preprocessing is to improve the image in ways that increase the chances for successes of the other processes. Preprocessing typically deals with techniques for enhancing contrast, removing noise, and isolating regions whose texture indicate a likelihood of al-

phanumeric information [29].

In our work, after getting the palmprint images, we have to find the central region of interest from the whole palmprint which can be further used for feature extraction. Our objective here is to isolate the central part of the palm which consists of some unique textural as well as line information about an individual.

C. Histograms: The histogram of an image represents the frequency of occurrence of gray levels in the image. The histogram of an 8-bit binary image corresponds to a table with 256 entries, indexed from 0 to 255. Each entry records the number of occurrences of each level in the image. An image histogram can simply be computed by creating a table of size equivalent to the number of gray levels of the image, with table entries initialized to zero, each entry is incremented for a pixel in the image of that gray level value [29].

D. Edge and Boundary Detection: Edge detection is by far the most common approach for detecting meaningful discontinuities in gray level. An edge is the boundary between two regions with relatively distinct gray-level properties. Edge detection is an important operation in a large number of image processing applications such as image segmentation, character recognition, and scene analysis. An edge in an image is represented as connected pixels across which the brightness of the image changes abruptly in magnitude or in the rate of change of magnitude.

Canny edge detection is the most popular edge detection technique that is used in the field of image processing. It can be summarized by the following steps. First the image is smoothened with a Gaussian filter and then the edges are enhanced. The edges that are wide are thinned to achieve Non-maxima suppression. To reduce the number of edges and thereby reduce number of false detections a low threshold is applied to set all the values below this threshold to zero, and the edges above a high threshold are grown into contours by searching for candidate neighbor edge points [29].

2.4 Summary

In this section an overview of palmprint recognition systems including their different phases like image acquisition, preprocessing, feature extraction, matching etc. are discussed. Discussions on Hill cipher, modular arithmetic, and various modified Hill ciphers are made. Some concepts related to digital image processing which are involved in our work are also studied.

Chapter 3

Proposed Approach

Chapter 3

Proposed Approach

In this chapter we have proposed a preprocessing scheme which is a rotation and translation invariant, generates the central part of the palm that is the region of interest (ROI). Then after getting the ROI, they are stored in local or remote database for feature extraction. For maintaining the privacy of the palmprints of the users we have proposed a traditional encryption technique which is an advanced Hill Cipher which encrypts the palmprints and also the sub-images before transmission to remote databases or local database. Also it embeds some security to the palmprints.

3.1 The Model

Biometric authentication systems are widely applied because they offer inherent advantages over classical knowledge-based and token-based personal identification approaches. However, biometric systems are vulnerable to various attacks; such potential attacks must be analyzed before biometric systems are massively deployed in security systems. For example, they are open to database, replay, and brute-force attacks as discussed in Section 2.2.

Cryptography is one possible solution that would allow us to better defend against replay, brute force and database attacks. Systems protected by cryptography store and transmit only encrypted templates in databases and through data links. We have proposed a cryptographic approach for encrypting the palmprint images to protect the privacy of the users and also to embed security into the

palmprint images. Our proposed model is shown in Figure 3.1.

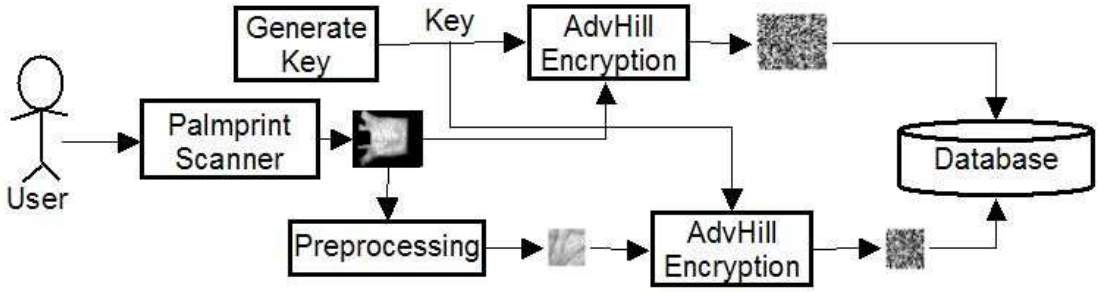

Figure 3.1: Proposed model for Privacy and Security of Palmprints

3.2 Palmprint Image Preprocessing

The goal of preprocessing is to obtain a sub-palmprint image for feature extraction and to eliminate the variation caused by rotation and translation. This preprocessing method is a modification of the approaches, proposed by W. Li et al. [6] and X. Su et al. [7]. In fact, our approach is similar to these two preprocessing methods.

3.2.1 The Algorithm

The five main steps of the proposed preprocessing algorithm are given below and shown pictorially in Figure 3.2.

Step 1: Apply a lowpass filter to the original image. Then, use a threshold, K_{th}, to convert this original image to a binary image as shown in Figure 3.2(b). Mathematically, this transformation can be represented as

$$I_B(x,y) = \begin{cases} 1, & \text{if } I_O(x,y) * F_L(x,y) > K_{th} \\ 0, & \text{if } I_O(x,y) * F_L(x,y) \geq K_{th} \end{cases} \tag{3.1}$$

Step 2: Extract the boundaries of the holes,$(B_i x_j, B_i y_j), (i = 1, 2)$, between fingers using a boundary tracking algorithm. The start points, (Sx_i, Sy_i), and end points, (Ex_i, Ey_i), of the holes are then marked in the process as shown in Figure 3.2(c).

Step 3: Compute the center of gravity, (Cx_i, Cy_i) of each hole with the following equations:

$$Cx_i = \frac{\sum_{j=1}^{N(i)} B_i x_j}{N(i)}, \; Cy_i = \frac{\sum_{j=1}^{N(i)} B_i y_j}{N(i)} \tag{3.2}$$

where $N(i)$ represents the number of boundary points of the hole i. Then, construct a line that passes through (Cx_i, Cy_i) and the midpoint of (Sx_i, Sy_i) and (Ex_i, Ey_i). The line equation is defined as

$$y = x\frac{Cy_i - My_i}{Cx_i - Mx_i} + \frac{My_i Cx_i - Mx_i Cy_i}{Cx_i - Mx_i} \tag{3.3}$$

where (Mx_i, My_i) is the midpoint of (Sx_i, Sy_i) and (Ex_i, Ey_i). Based on these lines, the key points, $(K_1, K_2,)$, can easily be detected as shown in Figure 3.2(d).

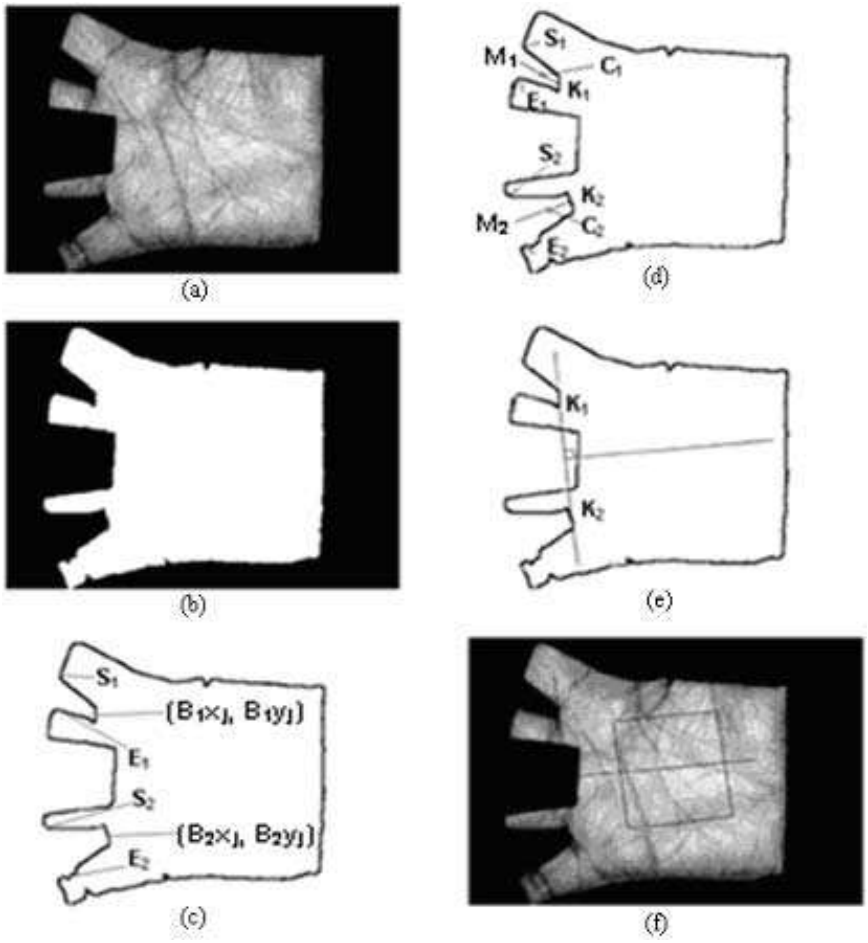

Figure 3.2: Main steps of preprocessing: (a) original image, (b) binary image, (c) boundary tracking, (d) key points (K_1 and K_2) detecting, (e) the coordinate system and (f) The central part (ROI) of a palmprint.

Step 4: Line up K_1 and K_2 to get the Y-axis of the palmprint coordinate system and make a line through their mid point which is perpendicular to the Y-axis, to determine the origin of the coordinate system as shown in Figure 3.2(e). This coordinate system can align different palmprint images.

Step 5: Extract a sub image with a fixed size on the basis of the coordinate system, which is located at a certain central part of the palmprint which is the ROI used for feature extraction. This is shown in Figure 3.2(f).

3.2.2 Simulations and Results

In the following experiment, palmprint images are collected from the PolyU palmprint database [30]. Figure 3.3 shows some of the palmprint images from PolyU database. To simulate our rotation as well as translation invariant image preprocessing scheme, we have manually rotated the palmprint images to different angles around 1 to 10 degrees both clockwise and counterclockwise. Then we preprocessed the various images and our generated central parts are found similar for all the rotated images of the same original palmprint.

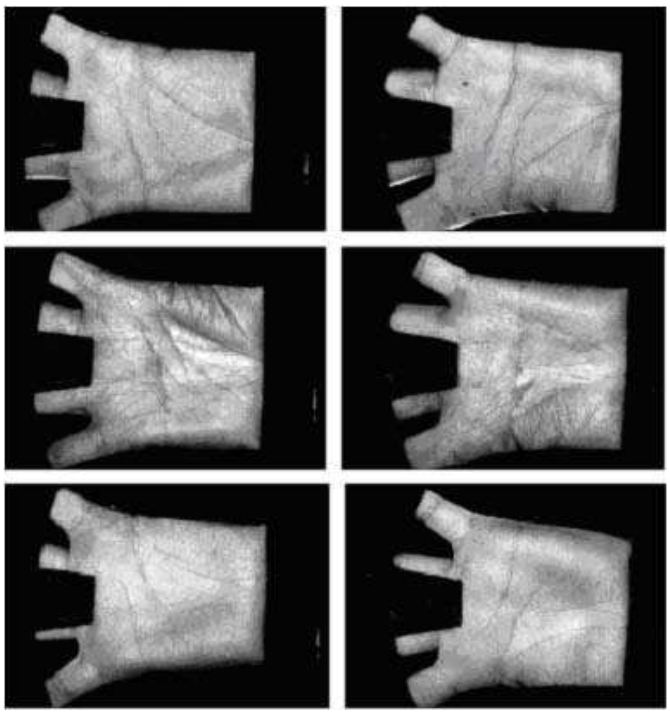

Figure 3.3: Palmprint images from PolyU Database

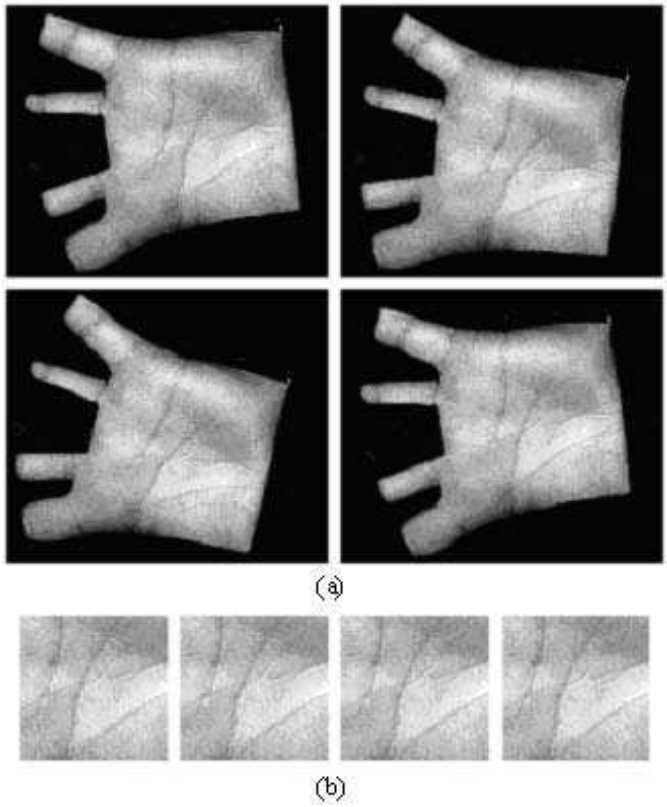

Figure 3.4: (a) Rotated input palmprint images for preprocessing and (b) output generated central parts of the image

Figure 3.4 shows the rotated input images and output generated central parts of the image which are similar. As we have considered the centre of gravity of the two holes of the palmprint image, if the image is rotated, still the centre of gravity of the holes remain same. As the new coordinate system is based on that centre of gravity of the holes, if the image is translated a small distance also, the result is same.

3.3 Privacy and Security of Palmprint Images

After the preprocessing is over, we get the central ROI part of the palmprint. Now our proposed approach is to maintain the privacy of and provide security to the palmprints of the users. For this we have proposed an advanced Hill Cipher algorithm which can be used for encrypting the palmprint images. The following sections explain our proposed approach.

3.3.1 Advanced Hill Cipher Algorithm(AdvHill)

The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. We note that Hill cipher can be adopted to encrypt gray-scale and colour images. For gray-scale images, the modulus will be 256 (the number of levels is considered as the number of alphabets). In the case of color images, first decompose the color image into (R-G-B) components. Second, encrypt each component (R-G-B) separately by the algorithm. Finally, concatenate the encrypted components together to get the encrypted colour image [27]. As our palmprint images are gray scale images, we concentrate on gray image encryption.

A main drawback of the Hill cipher algorithm is that it encrypts identical plaintext blocks to identical ciphertext blocks and cannot encrypt images that contain large areas of a single color. Thus, it does not hide all features of the image which reveals patterns in the plaintext. Despite Hill cipher being difficult to break with a ciphertext-only attack, it succumbs to a known plaintext attack assuming that the opponent has determined the value of p (number of alphabets) being used. We present a variant of the Hill cipher that we have named as AdvHill, which overcomes these disadvantages. Visually and computationally, experimental results demonstrate that the proposed variant yields higher security and significantly superior encryption quality compared to the original one. The algorithm and the block diagram (Figure 3.5) for AdvHill are given as follows.

The AdvHill Algorithm

Step 1. A self-invertible key matrix of dimensions m x m is constructed.

Step 2. The plain image is divided into m x m symmetric blocks.

Step 3. The i^{th} pixels of each block are brought together to form a temporary block.

- **a.** Hill cipher technique is applied onto the temporary block.
- **b.** The resultant matrix is transposed and Hill cipher is again applied to this matrix.

Step 4. The final matrix obtained is placed in the i^{th} block of the encrypted image.

Step 5: The steps 3 to 4 are repeated by incrementing the value of i till the whole image is encrypted.

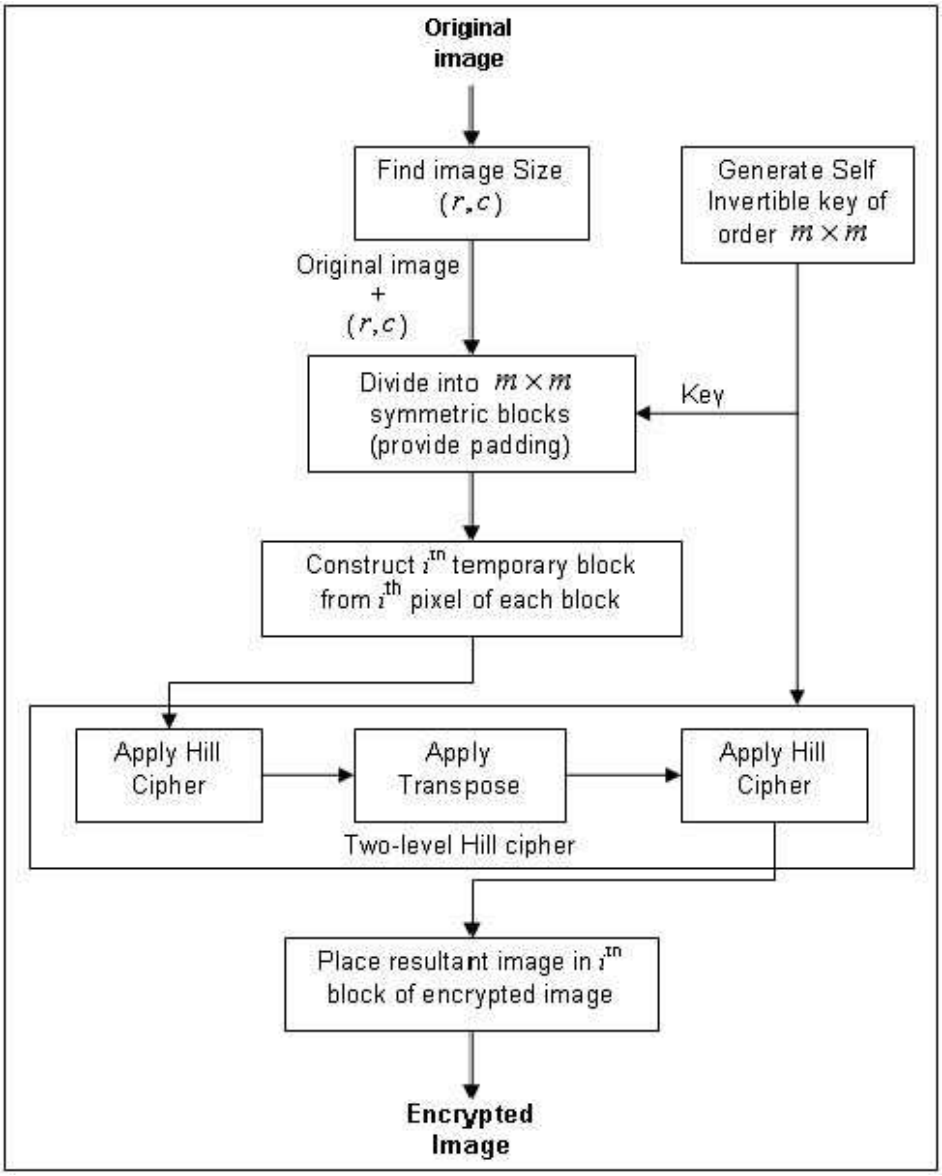

Figure 3.5: Block Diagram for proposed AdvHill Cipher Encryption

We have taken different images and encrypted them using the original cipher and our AdvHill algorithm and the results are shown below in Figure 3.6. It is clearly noticeable from the Figure 3.6(h,i), that original Hill cipher algorithm could not be able to decrypt the images properly because of the background of the

image of same colour or gray level. But our proposed AdvHill cipher algorithm could decrypt the images properly as shown in Figure 3.6(m,n). This shows that our image encryption scheme is stronger than the original Hill cipher and is also resistant to known-plaintext attack. Figure 3.7 shows the time analysis for Lena image encryption by original Hill and AdvHill algorithms. It is clear that our AdvHill takes more time than that of original Hill to encrypt the image but with stronger security. Figure 3.8 and 3.9 show how our AdvHill algorithm is capable of decrypting the image as in the histograms it introduces more gray levels which leads to failure of frequency analysis by attackers.

3.3.2 Palmprint Image Encryption using AdvHill

From the previous section, it is clear that our AdvHill cipher algorithm works well for image encryption compared to that of original Hill Cipher algorithm. We can apply our AdvHill to any type of images for encryption. So to provide security and maintain privacy of the palmprints of the users, we encrypt the palmprint images and sub-images and then transmit through communication links or store in databases for feature extraction. Before feature extraction, the palmprint sub-images are decrypted by the same key as the key matrix is a self-invertible matrix.

3.3.3 Simulations and Results

We applied our AdvHill cipher algorithm to original palmprint images and also the cropped palmprint sub-images for encryption. The results are shown in Figure 3.10 and 3.11.

3.4 Summary

In this chapter a new preprocessing scheme has been proposed which is both rotation as well as translation invariant. Then a cryptographic approach is proposed for encrypting the palmprint images and also the sub-images for maintaining the privacy of and adding security to the palmprint images of the users. The experimental results then discussed for both the proposed approaches.

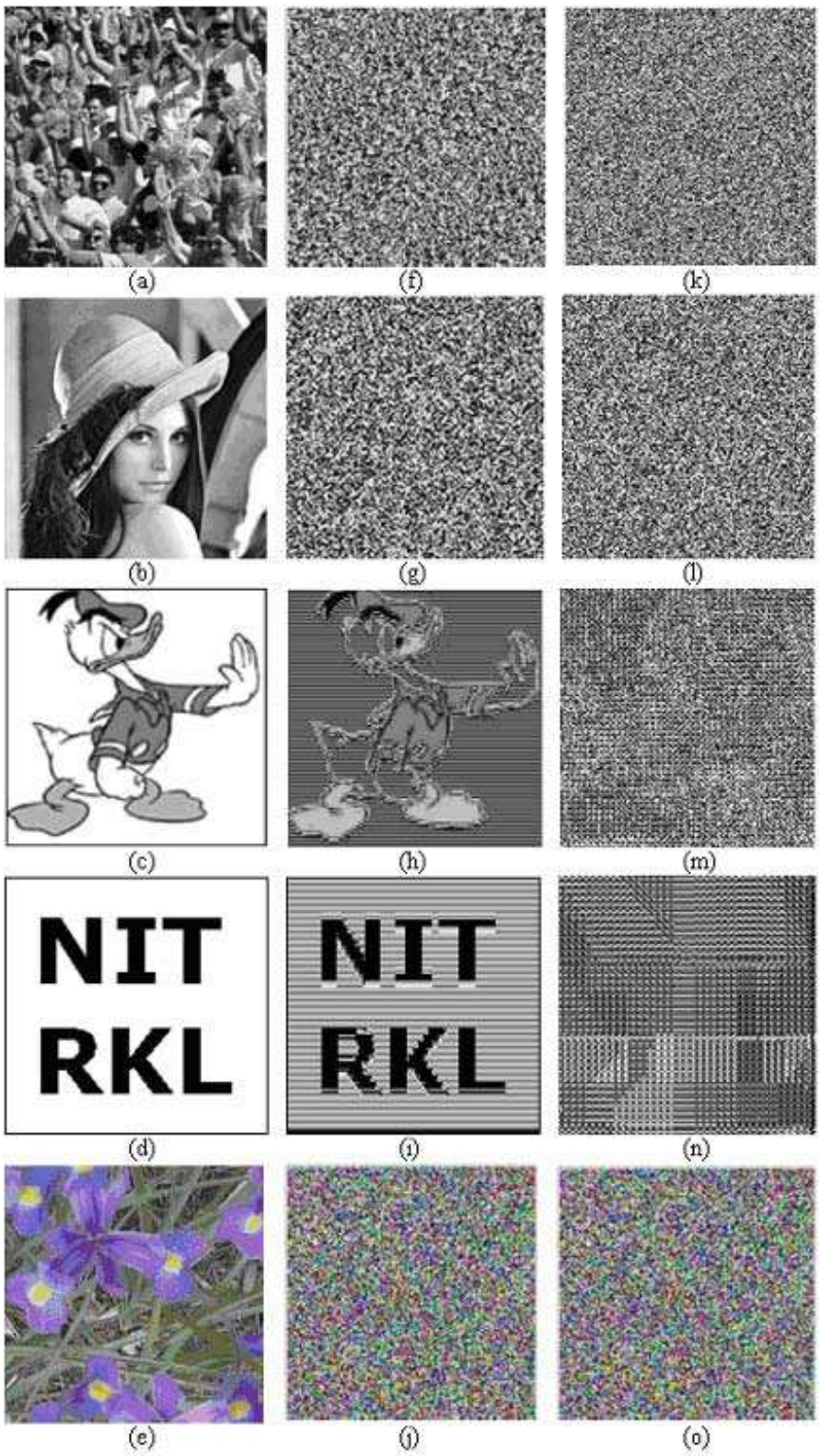

Figure 3.6: Original images (a-e), corresponding encrypted images by Hill Cipher (f-j) and by AdvHill Cipher Algorithm (k-o).

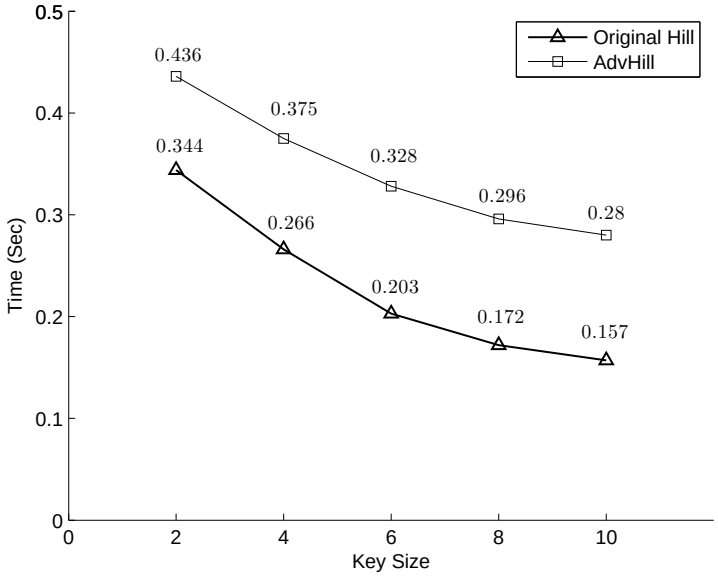

Figure 3.7: Encryption time test of Lena image

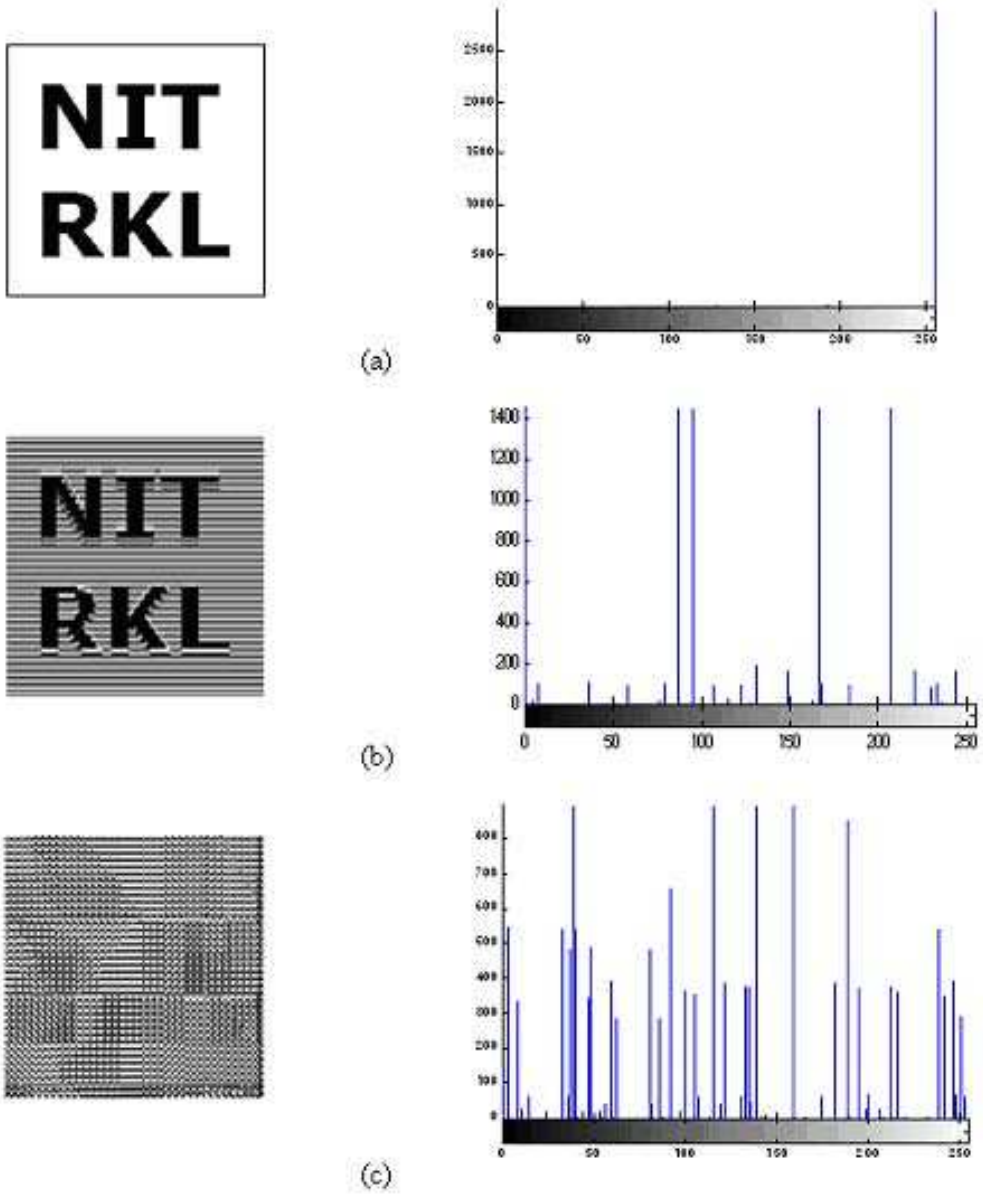

Figure 3.8: Histograms of (a) original nitrkl image (b) nitrkl image encrypted by original Hill cipher and (c) nitrkl image encrypted by AdvHill cipher

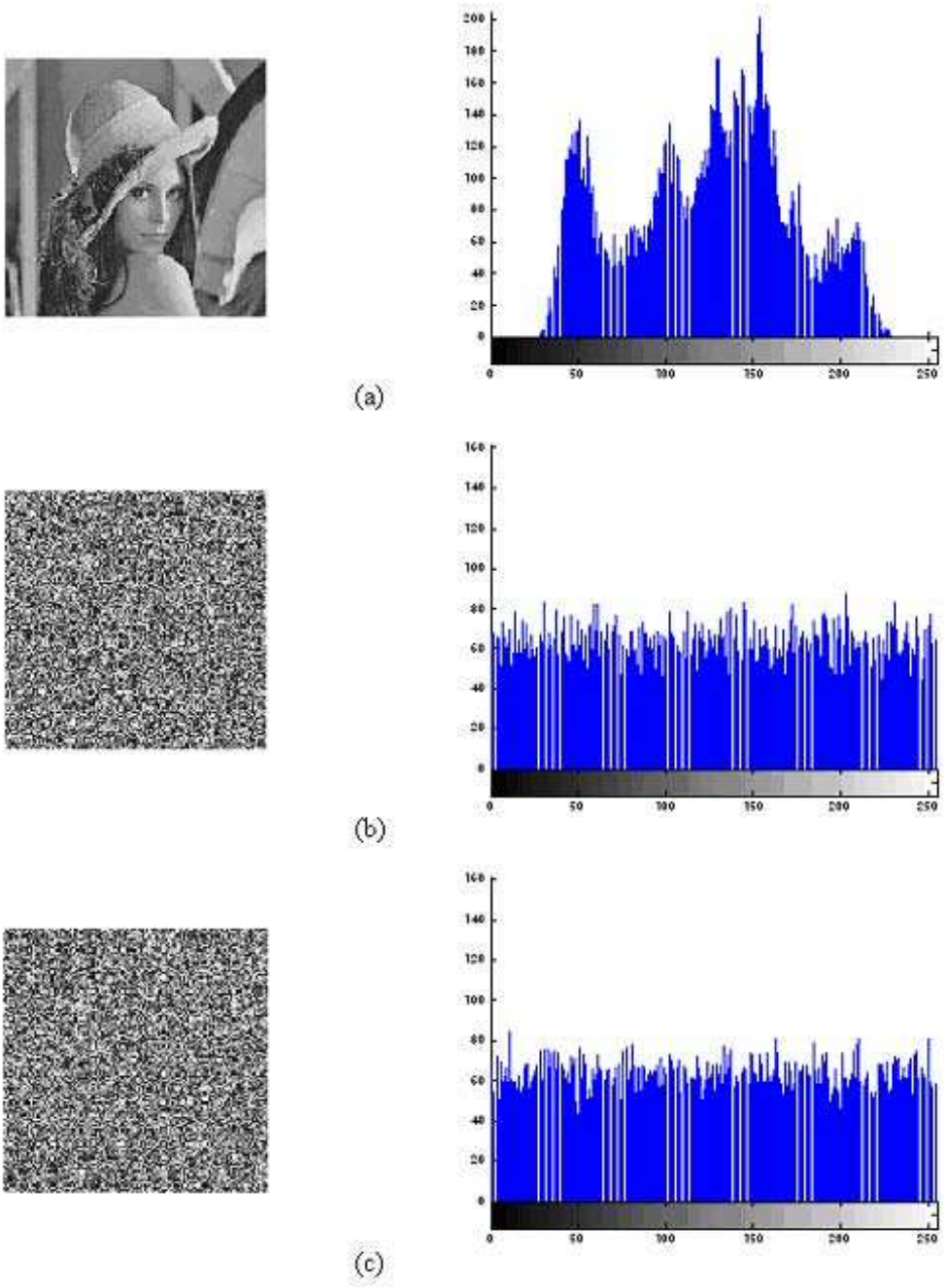

Figure 3.9: Histograms of (a) Lena original image (b) Lena image encrypted by original Hill cipher and (c) Lena image encrypted by AdvHill cipher

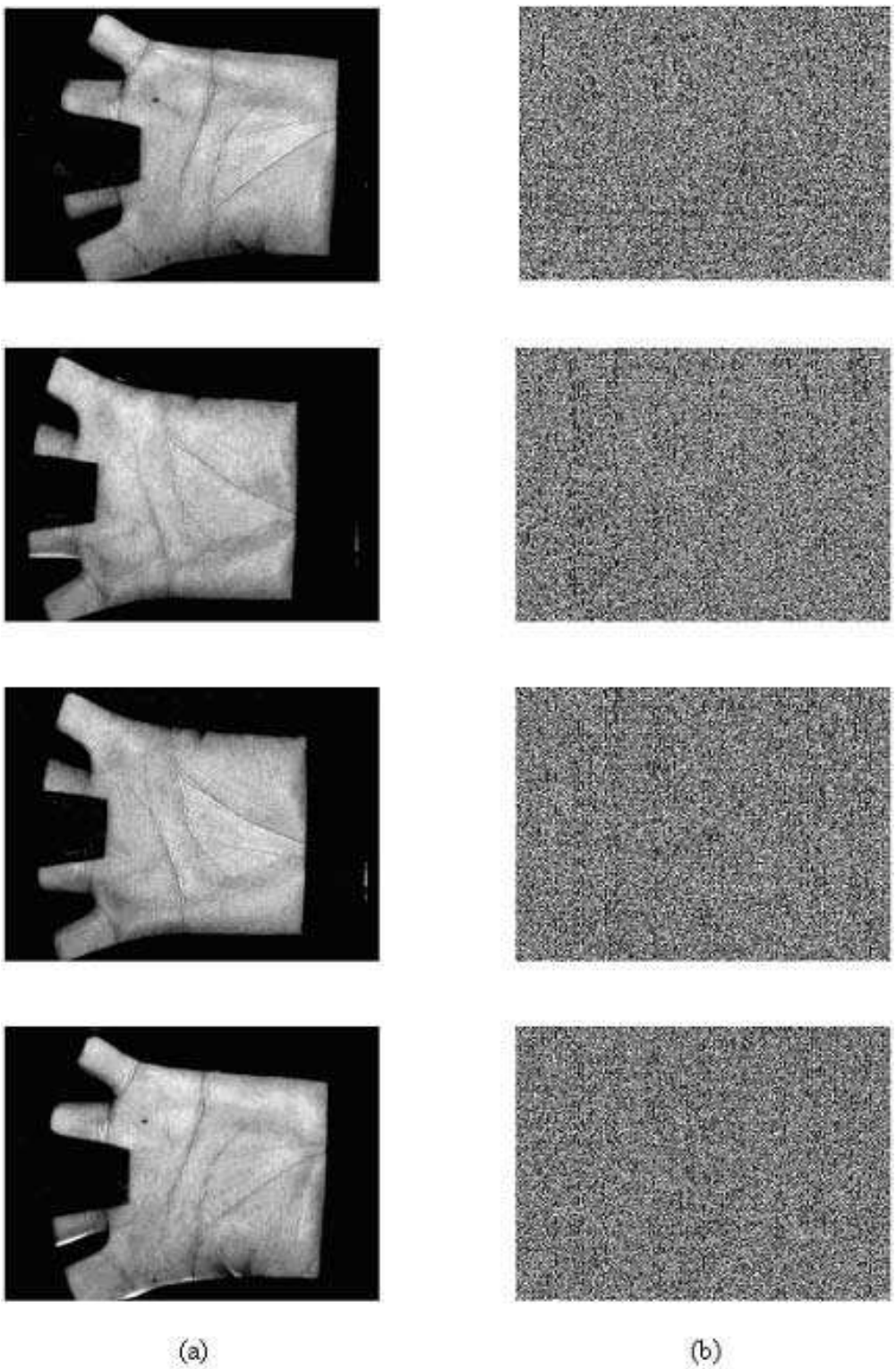

Figure 3.10: (a) the original palmprint images (b) encrypted palmprints by AdvHill cipher algorithm

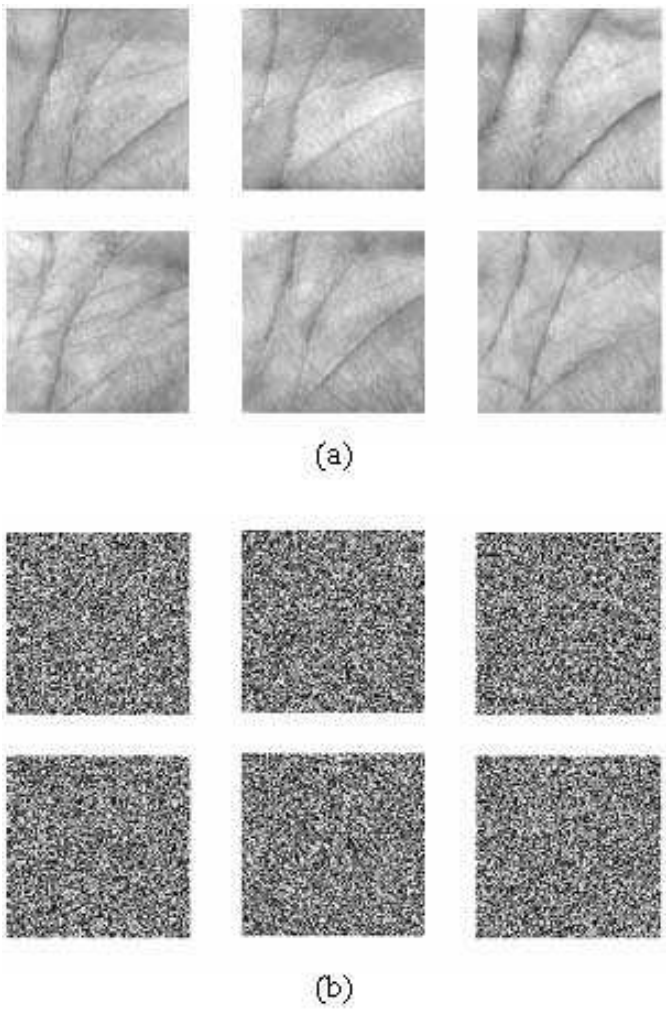

Figure 3.11: (a) palmprint sub-images after preprocessing and (b) their corresponding encrypted images by AdvHill algorithm

Chapter 4

Conclusions

Conclusions

Further Development

Chapter 4

Conclusions

Biometrics plays an important role in personal identification. The importance of biometrics in everyday life has been discussed and different biometric technologies are introduced. It has been shown that palm can also be a good biometric. The work reported in this thesis is summarized in this chapter. Section 4.1 lists the pros and cons of the work. Section 4.2 provides some scope for further development.

4.1 Achievements and Limitations of the work

In this thesis, various palmprint recognition systems are studied and a palmprint preprocessing scheme is proposed. As we have considered the centre of gravity of the two holes of the palmprint image, the palmprint images will not suffer due to rotation and translation of the palms during enrollment and verification or identification phases. The privacy of the palmprints is protected and also the palmprint images and sub-images can be sent and stored in remote databases securely, as those are encrypted using an advanced version of Hill Cipher algorithm which can resist replay, database and brute force attacks.

We have proposed a cryptographic which is a traditional method of encrypting images. Systems protected by cryptography store and transmit only encrypted templates in databases and through data links. However, cryptography is not suitable for speed-demanding matching, e.g. real-time large-scale identification, since decryption is required before matching. Another potential solution is cancellable biometrics which can be used for encryption. Cancellable biometrics transform

original templates into other domains and perform matching in the transformed domain.

4.2 Further Development

Although cancellable biometrics overcome the weakness of cryptography, current cancellable biometrics are still not secure enough for the palmprint identification. For example, attackers can still insert stolen templates replay and database attacks before systems can cancel the stolen templates and reissue new templates. Furthermore, current cancellable biometrics cannot detect replay and database attacks. In other words, if attackers insert unregistered templates into data links or databases, systems cannot discover the unregistered templates. To solve these problems, we can take advantages of cryptography and cancellable biometrics to design a set of security measures to prevent replay, brute force and database attacks for secure palmprint identification.

Bibliography

[1] N. Frykholm. Passwords: Beyond the terminal interaction model, 2000. University of Umea.

[2] Miller G. A. The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological Review*, 63:81–97, 1956.

[3] Salil Prabhakar Anil K. Jain and Lin Hong. A multichannel approach to fingerprint classification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 21(4):348–359, 1999.

[4] Salil Prabhakar Sharath Pankanti and Anil K. Jain. On the individuality of fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(8):1010–1025, 2002.

[5] D. Zhang and W. Shu. Two novel characteristics in palmprint verification: Datum point invariance and line feature matching. *Pattern Recognition*, 32(4):691–702, 1999.

[6] David Zhang Wenxin Li and Zhuoqun Xu. Palmprint identification by fourier transform. *International Journal of Pattern Recognition and Artificial Intelligence*, 16(4):417–432, 2002.

[7] Ding Tianhuai Su Xiaosheng, Lin Xirong and et al. Palmprint feature extraction based on wavelet transform. *Tsinghua Univ(Sci and Tech)*, 43(8):1049–1051,1055, 2003.

[8] K.C. Fan C. C. Han, H. L. Cheng and C. L. Lin. Personal authentication using palmprint features. *Pattern Recognition (Special issue: Biometrics)*, 36(2):371–381, 2003.

[9] David Zhang Wai Kin Kong and Wenxin Li. Palmprint feature extraction using 2-d gabor filters. *Pattern Recognition*, 36:2339–2347, 2003.

[10] Jun ying Gan and Dang pei Zhou. A novel method for palmprint recognition based on wavelet transform. In *The IEEE Proceedings of International Conference on Signal Processing (ICSP2006)*, volume 3, 2006.

[11] Kuanquan Wang Xiangqian Wu and David Zhang. Palmprint texture analysis using derivative of gaussian filters. In *The IEEE Proceedings of International Conference on Computational Intelligence and Security (ICCIS2006)*, volume 1, pages 751–754, 2006.

[12] Michael M. Bronstein Alexander M. Bronstein and Ron Kimmel. Three-dimensional face recognition. *International Journal of Computer Vision*, 64(1):5–30, 2005.

[13] Yossi Zana and Jr Roberto M. Cesar. Face recognition based on polar frequency features. *ACM Transactions on Applied Perception*, 3(1):62–82, 2006.

[14] Jinsu Choi Jaemin Kim, Seongwon Cho and II Robert J. Marks. Iris recognition using wavelet features. *Journal of VLSI Signal Processing*, 38(2):147–156, 2004.

[15] Kevin W. Bowyer Xiaomei Liu and Patrick J. Flynn. Experimental evaluation of iris recognition. In *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, volume 3, page 158, Washington, DC, USA, 2005. IEEE Computer Society.

[16] Hui Chen and Bir Bhanu. Contour matching for 3d ear recognition. In *Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05)*, volume 1, pages 123–128, Washington, DC, USA, 2005. IEEE Computer Society.

[17] Tee Connie Andrew Teoh Beng Jin Michael Goh Kah Ong and David Ngo Chek Ling. A single-sensor hand geometry and palmprint verification system. In *Proceedings of the 2003 ACM SIGMM workshop on Biometrics Methods and Applications (WBMA'03)*, pages 100–106, New York, NY, USA, 2003. ACM Press.

[18] Judith A. Markowitz. Voice biometrics. *Communications of the ACM*, 43(9):66–73, 2000.

[19] M. Gifford and N. Edwards. Trial of dynamic signature verification for a real-world identification solution. *BT Technology Journal*, 23(2):259–266, 2005.

[20] Aykut Guven and Ibrahim Sogukpinar. Understanding users' keystroke patterns for computer access security. *Computers and Security (Elsevier)*, 22(8):695–706, 2003.

[21] J. You D. Zhang, W. K. Kong and M. Wong. On-line palmprint identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1041–1050, 2003.

[22] David Zhang Adams W. K. Kong and Mohamed Kamel. Analysis of brute-force break-ins of a palmprint authentication system. *IEEE Transactions On Systems, Man and Cybernetics-Part B: Cybernetics*, 36(5):1201–1205, 2006.

[23] J. H. Connell R. M. Bolle and N. K. Ratha. Biometric perils and patches. *Pattern Recognition*, 35:2727–2738, 2002.

[24] William S. Stallings. *Cryptography and Network Security.* Prentice Hall, 4th edition, 2005.

[25] B. Acharya and et. al. Novel methods of generating self-invertible matrix for hill cipher algorithm. *International Journal of Security*, 1(1):14–21, 2007.

[26] S Saeednia. How to make the hill cipher secure. *Cryptologia*, 24(4):353–360, 2000.

[27] Amin M. Ismail I. A. and Diab H. How to repair the hill cipher. *International Journal of Zhejiang Univ. Science A*, 7(12):2022–2030, 2006.

[28] Y. RANGEL-ROMERO and et. al. Comments on how to repair the hill cipher. *Journal of Zhejiang University SCIENCE A*, pages 1–4, 2007.

[29] Richard E. Gonzalez Rafael C. Woods. *Digital Image Processing*. Prentice Hall, 2nd edition, 2002.

[30] PolyU Palmprint Database. http://www.comp.polyu.edu.hk/ biometric.

[31] Shujun Li and Xuan Zheng. On the security of an image encryption method. In *Proceedings of 2002 IEEE International Conference on Image Processing (ICIP 2002)*, volume 2, pages 925–928, 2002.

Dissemination of Work

1. S. K. Panigrahy, D. Jena, and S. K. Jena, ‶A Rotational- and Translational-Invariant Palmprint Recognition System″, Published in *International Conference on Data Engineering and Management (ICDEM-2008)*, 9 February, 2008, Tiruchirapalli, Tamilnadu, India, pp 294 - 297, 2008.